PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/32, H04N 1/32

A1

(11) International Publication Number: **WO 00/35144**

(43) International Publication Date: 15 June 2000 (15.06.00)

(21) International Application Number: PCT/EP99/09576

(22) International Filing Date: 7 December 1999 (07.12.99)

(30) Priority Data:
98204136.0 8 December 1998 (08.12.98) EP

(71) Applicant *(for all designated States except US)*: IRDETO ACCESS B.V. [NL/NL]; Jupiterstraat 42, NL–2132 HD Hoofddorp (NL).

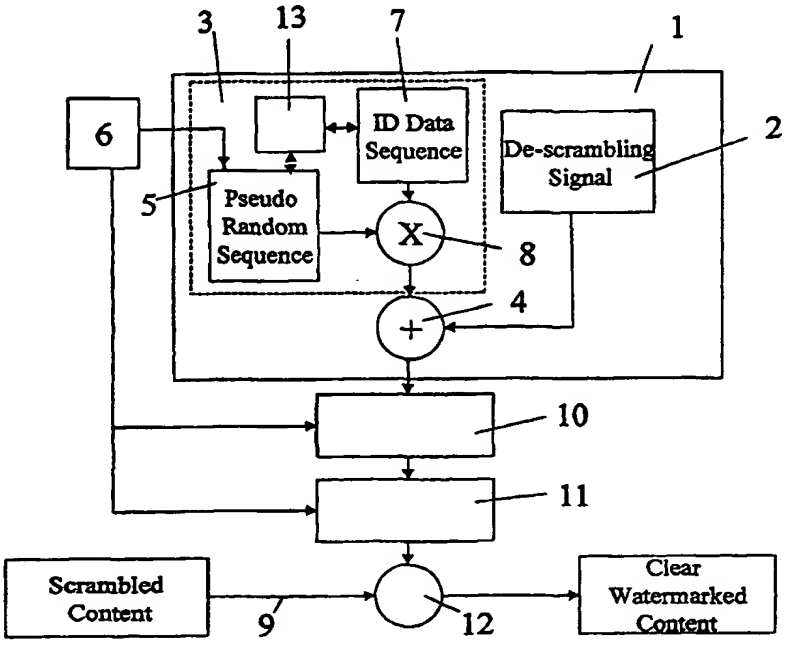
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: WAJS, Andrew, Augustine [GB/NL]; Schotersingel 93, NL–2023 AA Haarlem (NL).

(74) Agent: DE VRIES, Johannes, Hendrik, Fokke; De Vries & Metman B.V., Overschiestraat 180, NL–1062 XK Amsterdam (NL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DEVICE FOR GENERATING A DESCRAMBLING SIGNAL



(57) Abstract

A device for generating a descrambling signal comprises a first generator providing a descrambling base signal, a second generator providing a watermark signal, and means for combining the descrambling base signal and the watermark signal into a descrambling signal. The watermark signal generated by the second generator includes a device identification.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Device for generating a descrambling signal

The invention relates to a device for generating a descrambling signal.

Such a device is used in a descrambling system for descrambling a scrambled content or information signal. When the content is descrambled the clear content could be used by unauthorized persons, i.e. a pirate, for distribution or other unauthorized commercial purposes. With conventional systems for descrambling a scrambled content, it is generally impossible to trace the descrambling system or descrambling signal generating device which is used to obtain the content distributed by an unauthorized person.

The invention aims to provide a device of the above-mentioned type, wherein it is relatively easy to trace the descrambling system or descrambling signal generating device used to obtain a clear content, by means of this clear content.

To this end the device of the invention comprises a first generator providing a descrambling base signal, a second generator providing a watermark signal, and means for combining the descrambling base signal and the watermark signal into a descrambling signal, wherein the watermark signal generated by the second generator includes a device identification.

In this manner a device is obtained, wherein the descrambling signal contains a watermark signal including a device identification. This device identification will be added to the clear content during the descrambling operation and in this manner the device can be traced by analysing the clear watermarked content.

The invention will be further explained by reference to a drawing showing a descrambling system equipped with an embodiment of the device of the invention.

In the following description an embodiment of a device for generating a descrambling signal will be described as used in a descrambling system described in a co-pending patent application of the same applicant. However it is noted that the present device for generating a descrambling signal is not restricted to a device for use in such a descrambling system.

The descrambling system shown in the drawing is provided with a device for generating a descrambling signal which is preferably part of a secure device 1, such as a smart card. The descrambling signal generating device comprises a first generator 2 providing a descrambling base signal and a second generator 3 providing a watermark signal, wherein the descrambling base signal and the watermark signal are combined in an adder 4. The adder 4 provides the descrambling signal used in the descrambling system which will be described hereinafter. It is noted that the term descrambling base signal is used to refer to any conventional descrambling signal.

In the preferred embodiment, the second generator 3 comprises a pseudo random sequence generator 5 seeded by a key received from a control unit 6 of the descrambling system. The second generator 3 further comprises a device identification sequence source 7, which can be made as a memory. The identification sequence is modulated on the pseudo random sequence provided by the generator 5 by means of an exclusive or operation 8. The bit rate of the pseudo random sequence is much higher than the bit rate of the identification sequence, so that the output of the exclusive or operation 8 has a bandwith corresponding with the bit rate of the pseudo random sequence. The output of the exclusive or operation 8 is the watermark signal which is added to the descrambling signal.

The output of the adder 4 is the descrambling signal which is used to descramble the scrambled input received on an input 9. As this scrambled input has been compressed and decompressed, an equalizer or compensation filter 10 is provided to replicate the impulse response of the transfer

function of this compression and decompression steps. The equalizer 10 is adjusted by the control unit 6 to provide the correct impulse response. This is further described in the above-mentioned co-pending application. Further the output of the equalizer 10 is processed by a processor 11 in such a manner that the entropy distribution of the descrambling signal corresponds to the entropy distribution of the original scrambling signal and clear content. The processor 11 is also adjuted by the control unit 6. It is noted that information on the required settings can be received by the control unit 6 from an outside source as part of an entitlement or other control file, for example. This file can be forwarded as a separate data stream or can be inserted into the scrambled information data stream. By combining the scrambled content and the processed descrambling signal in a descrambler 12 a clear watermarked content is obtained. The decrambling system is not a part of the present invention and is described in the co-pending application which is deemed to be incorporated here by reference.

If the descrambling signal generating device is used by a pirate to obtain the clear content, this clear content will be watermarked with the device identification sequence. By analysing the content provided by the pirate, the watermark signal can be detected and in this manner the secure device 1 used by the pirate can be traced. Thereafter, the secure device can be made useless, for example by no longer using the private key of the secure device 1 for encrypting the files containing information necessary for operating the descrambling system, such as an entitlement file, the key for seeding the first generator 1 and the key for seeding the generator 5.

In order to prevent removal of the device identification sequence by combining the descrambling signals obtained from two or more descrambling signal generating devices, a processor 13 of the secure device 1 is programmed such that the phase relationship between the pseudo random sequence provided by the generator 5 and the device identification sequence provided by the source 7 is randomly se-

lected. This means that there is no fixed relationship between these two sequences if the output signals of two or more of the devices as described are combined. Averaging the output signals will then not result in a removal of the device identification sequences.

As an alternative, the processor 13 can control the exclusive or operation 8 on the device identification sequence and the pseudo random sequence such, that the device identification sequence is repetitively modulated on the pseudo random sequence, wherein at each repetition the processor 13 checks a next bit of the identification sequence and inverts all bits of the identification sequence if this checked bit has a given logic value, i.e. either a zero or a one. This means that if at the first repetition the first bit is a logic one for example, all bits are inverted. For the second repetition, the second bit is checked and if it is logic one, then the entire identification sequence is inverted, etc. Again averaging of the descrambling signals generated by the device described will not lead to removal of the device identification sequences.

If it is found that a device is used by a pirate to descramble a scrambled content for unauthorized commercial purposes, for example distribution on the internet, the provider of the descrambling signal devices, i.e. the secure devices, can trace the or each secure device used in an easy manner. For, the authorized person knows the pseudo random sequence generator used in the devices 1. By synchronising the pseudo random sequence with the watermarked content signal, the device identification sequence can be found. The manner for synchronisation corresponds with synchronisation in a spread spectrum system. Therefore, this synchronisation and detection of the watermark signal is not further described.

In case of a device as described using random selection of the phase relationship between the pseudo random sequence and the device identification sequence, it can easily be established from the symbol rate of the watermark signal how many sequences have been averaged. For, the data

rate of the device identification sequence is known to the authorized provider. If for example two identification sequences are contained in the watermarked content, it is possible to "de-multiplex" the two device identification sequences by selecting every second symbol detected for each identification sequence. Of course, first the "multiplex" of the two identification sequences is detected by synchronising the known pseudo random sequence with the watermarked clear content.

In case of devices using repeated insertion of the identification sequence into the pseudo random sequence with inversion of the bits depending on the bit value of each next bit, the identification sequences of the devices used to average out the watermark signals can be derived from the detected sequences hidden in the content. Assume for example that two devices have been used by the pirate having the identification sequences 101 and 110 and that these sequences are inserted four times with inversion of the bits as described. This means that the first device will have generated 101, 010, 101, 010, while the second device will have generated 110, 001, 001 and 110. Despite averaging these sequences, detection will provide the sequences 1xx, 0xx, x01, x10, wherein a "1" or a "0" occurs when there is coincidence of the same value and a "x" denotes an undetected symbol due to averaging out. As the provider knows the repetition and inversion scheme used, the detected sequences learn that the both sequences start with a value 1, as the first detected sequence starts with a value 1. Further, the second and third symbols of the sequences are not equal to each other. The second sequence provides no further information and the third sequence learns that the second symbol of only one identification sequence changed, so that we have 11x and 10x. The fourth detected sequence learns that the third symbol of at least one identification sequence changed again. If we assume one identification sequnce to be 101, this automatically provides 110 for the other.

It is noted that the above-described devices for

adding a watermark signal with random phase relationship or repeated insertion of the watermark signal can be used in combination with any type of descrambling signal generator or even separate from a descrambling signal generator.

A pirate could try to prevent watermark signal detection by slightly changing the bit rate of the content. As the provider knows the original bit rate of the content this type of distortion of the content to prevent watermark signal detection can be removed by comparing the bit rates of the original and pirate contents. The provider can then change the bit rate of the pirate content back to the original one and can then start one of the described detection schemes.

A further or other type of protection against unauthorized use by pirates can be obtained by using the processor 13 of the secure device 1 to add a compression hindering signal to the output of the generator 2. This compression hindering signal will then be part of the descrambling signal used by the descrambler 12 and will be inserted in this manner into the clear content on the output. The compression hindering signal for example inserts noise into the information signal which will not affect the quality of the information signal. It will however significantly affect any compression algorithm to effectively compress the information signal, so that a pirate will not be able to effectively recompress the clear content for distribution purposes. If the compression hindering signal is used independent of a descrambling signal generator, the compression hindering signal will be added to the clear content in a suitable manner.

The invention is not restricted to the above described embodiment which can be varied in a number of ways within the scope of the claims.

CLAIMS

1. Device for generating a descrambling signal, comprising a first generator providing a descrambling base signal, a second generator providing a watermark signal, and means for combining the descrambling base signal and the watermark signal into a descrambling signal, wherein the watermark signal generated by the second generator includes a device identification.

2. Device according to claim 1, wherein the watermark signal generator comprises a pseudo random sequence generator seeded by a key, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal.

3. Device according to claim 2, wherein the modulator provides an exclusive or operation on the device identification sequence and the pseudo random sequence, wherein preferably the bit rate of the pseudo random sequence is much higher than the bit rate of the device identification sequence.

4. Device according to claim 2 or 3, wherein the key delivered to the pseudo random sequence generator is received from an outside source.

5. Device according to any one of the preceding claims, comprising a generator for generating a compressing hindering signal and means for inserting the hindering signal into the descrambling signal.

6. Device according to any one of the preceding claims, comprising a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the phase relationship between the pseudo random sequence and the device identification sequence is randomly selected.

7. Device according to any one of claims 1-5, comprising, a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the device identification sequence is repetitively modulated on the pseudo random sequence, wherein at each repetition a control unit checks a next bit of the device identification sequence and inverts the bits of the device identification sequence if this bit has a given logic value.

8. Device for generating a watermark signal, comprising a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the phase relationship between the pseudo random sequence and the device identification sequence is randomly selected.

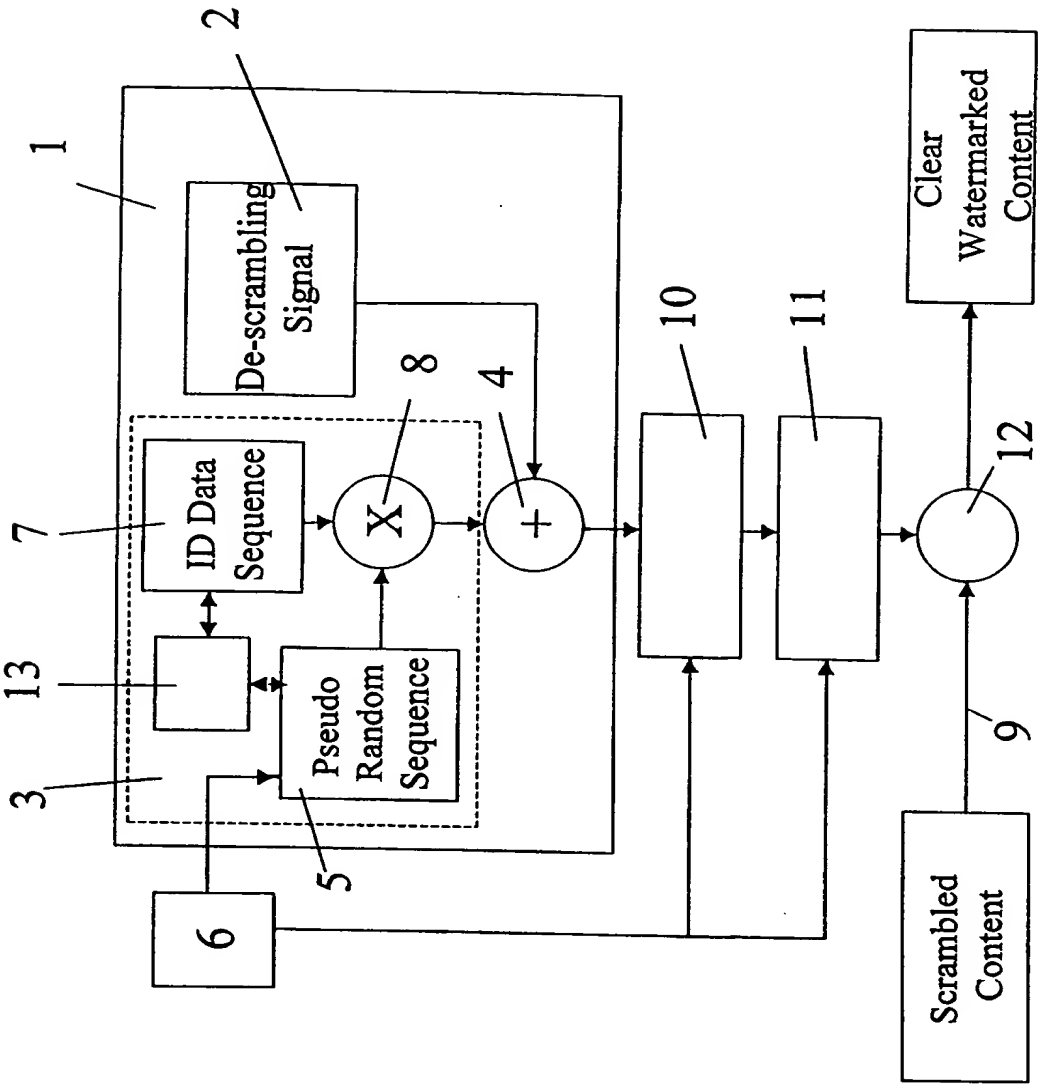
9. Device for generating a watermark signal, comprising a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the device identification sequence is repetitively modulated on the pseudo random sequence, wherein at each repetition a control unit checks a next bit of the device identification sequence and inverts the bits of the device identification sequence if this bit has a given logic value.

10. Device according to any one of the preceding claims, wherein the device is implemented in a secure device, such as a smart card.

11. System to detect a watermark signal hidden in an information signal, comprising a pseudo random signal generator, means for synchronising the pseudo random signal generator and the information signal, means for detecting a data sequence hidden in the information signal and for determining the number (n) of watermark signals in the hidden data sequence and means for selecting every n^{th} bit from the

detected hidden data sequence as bits of one of the n watermark signals.

12. System according to claim 11, wherein said means for determining the number (n) of watermark signals comprises means for detecting the bit rate of the hidden data sequence and comparing the detected bit rate with the known bit rate of one watermark signal.


1
2
De-scrambling Signal
ID Data Sequence
7
X
8
+
4
10
11
Clear Watermarked Content
12
13
Pseudo Random Sequence
3
5
6
9
Scrambled Content

INTERNATIONAL SEARCH REPORT

Internat. Application No
PCT/EP 99/09576

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 809 139 A (GIROD ET AL.) 15 September 1998 (1998-09-15) column 1, line 63 -column 2, line 8 column 10, line 44 -column 11, line 9	1
A	EP 0 493 053 A (XEROX) 1 July 1992 (1992-07-01) abstract column 5, line 34 - line 42	8,9
A	US 4 528 588 A (LOEFBERG BO) 9 July 1985 (1985-07-09) column 9, line 13 -column 11, line 55	1

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 March 2000	05/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat. Application No
PCT/EP 99/09576

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 840 513 A (NIPPON ELECTRIC CO) 6 May 1998 (1998-05-06) column 4, line 7 - line 16 column 6, line 1 - line 16 column 7, line 4 -column 8, line 8 column 11, line 10 - line 48	11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internati Application No
PCT/EP 99/09576

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5809139	A	15-09-1998	NONE		
EP 493053	A	01-07-1992	US	5315098 A	24-05-1994
			DE	69119882 D	04-07-1996
			DE	69119882 T	28-11-1996
			JP	2060237 C	10-06-1996
			JP	4334266 A	20-11-1992
			JP	7097822 B	18-10-1995
US 4528588	A	09-07-1985	SE	418656 B	15-06-1981
			AT	19320 T	15-05-1986
			AU	547877 B	07-11-1985
			AU	7641881 A	28-04-1982
			CA	1183950 A	12-03-1985
			DK	233682 A,B,	24-05-1982
			EP	0067998 A	05-01-1983
			FI	823651 A,B,	26-10-1982
			JP	57501899 T	21-10-1982
			NO	821727 A	25-05-1982
			WO	8201273 A	15-04-1982
			US	4595950 A	17-06-1986
EP 0840513	A	06-05-1998	US	5915027 A	22-06-1999
			AU	4434097 A	07-05-1998
			CA	2219205 A	05-05-1998
			JP	10145757 A	29-05-1998
			SG	63773 A	30-03-1999